Secure Cloud Data Using Attribute Based Encryption

Miss. Chopade Sonali S.[1], Miss. Bade Prachi N.[2], Miss. Bagal Shweta A.[3]

Miss.Kapurkar Megha E.[4]

BE Student of Department of Computer Science and Engineering ,AGTI'S Dr.Daulatrao Aher College of Engg, Karad, Maharashtra,India

Abstract*— Currently world there are many extra challenges for security of data and access handle when users outsource sensitive data for sharing on another party server known as cloud servers, which are not within the same trusted domain as data owners. The existing ideas used to maintain confidentiality of personal medical record (PMR) against untrusted servers by disclosing data decryption keys only to authorized users. However, in doing so, these answer inevitably introduce complexity in key management also burden on the data owner in data management well as in key management. The problem of simultaneously achieving security and data confidentiality and fine-grainedness of access control still remains unresolved. This paper addresses this challenge 1) Key management, 2) Defining and enforcing access policies based on data attributes, and, 3) Keyword search over the encrypted data. PMR(patient medical record)in the system users need to deal with complicated key the management problem to accomplish fine-grained access control when their PMRs are encrypted using symmetric key cryptography or asymmetric key cryptography and With our scheme multi-authority attribute based access control (MA-ABAC) we can reduce the key management complexity for owners and users. For this users are divided into the two domains; professional domain and personal domain. To achieve security of PMR, key management, user revocation and efficient keyword search exploiting KP-ABE, Multi-authority attribute based access control(MA-ABAC), and uniquely combining it with techniques of proxy re-encryption.

Keywords*— Attribute based encryption, Cloud computing, Fine-grained access control, KP-ABE, MA-ABAC, User Revocation, Proxy Re-encryption.

I. INTRODUCTION

Many companies have their maintenance and they provide lots of cloud computing services. More and more sensitive data from consumers have been concentrated into the cloud for its flexible management and economic savings. It is an exceptionally hard to look the most suitable services or products for ordinary consumers, as there are so many services and has turned out to be more pervasive, because of its advantages for consumers, including a products in cloud. It is very general that before outsourcing the sensitive data it is encrypted. It is difficult to encrypting full data first and then decrypting that data, due to the large bandwidth and computation burden. Consumers may need Cloud computing is a new trend of computing where resources like storage, computation poor, network, applications etc. are delivered as services. Pay-as-you-consume cloud computing paradigm to retrieve only certain specific dateless they are fascinated of the whole data collection. Cloud services provide great conveniences for the users to enjoy the on demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing.

1.1 Motivation

There are already well-known existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the users privacy. The existing systems define shared authority based privacy-preserving authentication protocol which allows security and privacy in the cloud storage. In this, shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations. Attribute based access control is adopted to realize that the user can only access its own data fields; proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users

1.2 Project Overview

In cloud it's a common practice to encrypt the data before it is been stored in cloud storage. Access control is another added security upon the encrypted data to be strongly stored in the cloud platform. At the start of the module while registering the user verification is checked through the OTP by Email. Attribute Based Encryption- ABE is finding its existence in cloud technology since it can deliver data privacy with one-to-many, fine grained and non-interactive access control.CP-ABE- Cipher text-policy attribute based encryption is a modified version of ABE with more flexibility in delivering security for general applications. Cloud service provider (CSP) manages all the servers and services provided to the client. The data owner can encrypt, decrypt, secure, store and share data to CSP. The files stored in cloud platform follow a hierarchical structure.

1.3 Need of Project

There square measure already well-known existing security solutions in the main specialize in the authentication to appreciate that a user's privative information cannot be unauthorized accessed, however neglect a refined privacy issue throughout a user difficult the cloud server to request different users for information sharing

II. LITERATURE SURVEY

Hong Liuet al. [1] explain Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, propose a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA,

JingiLi, Jinet al.[2] suggests a design to solve the problem of integrity auditing and secure deduplication on cloud data. Specifically, aiming at achieving both data integrity and de duplication in cloud, propose two secure systems, namely Sec Cloud and Sec Cloud+.Sec Cloud introduces an auditing entity with maintenance of a Map Reduce cloud, which helps clients generate data tags before uploading as ll as audit the integrity of data having been stored in cloud.

Prof. Rucha R. Galgali [3] investigated the problem related to the data privacy variousschemes are proposed based on the attribute based encryption techniques, still more attention is on privacy of the data content and the access control of the data and less attention is on the privilege control and the privacy of user's identity. In these presents Anony Control scheme which address data privacy as ll as users identity privacy also presents Anony Control-F for fully preventing the identity problems. In proposed scheme add user revocation in users to enable activating and deactivating users to enhance efficiency of system and adding more feasibility.

III. PROBLEM DEFINITION & SCOPE

A) Problem Statement

To provide security to the data on cloud by encrypting it by using Advanced Encryption Standard algorithm and Attribute Based Encryption scheme.

B) Reserch Scope

In our proposed system, we can store data securely on cloud by encrypting it using AES and ABE algorithms. Also, we can share data securely on cloud. Here, data is encrypted by sender by using public key and same can be decrypted at receiver side using private key. Therefore though the data is captured by hacker, he cannot decrypt is it until he gets private key, hence data is secure over the cloud.

C) Area of Reserch

Cloud computing is emerging paradigm provides various IT related services. The security and privacy are two major factors that inhibits the growth of cloud computing. Security factors are reasons behind lesser number real time and business relates cloud application compared to consumer related cloud application.Firstly,the pros and cons of different Attribute based encryption methods are analyzed.Secondly,a new encryption method based on Attribute Based Encryption (ABE) using hash function, digital signature and asymmetric encryption scheme has been proposed.Our proposed algorithm is simplified yet. efficient algorithm that can implemented for cloud critical application

.

The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications.

2.4 Goals and Objectives

i] To encrypt data and store on cloud to protect from hackers.
ii] For reliability and conventionality of cloud user.
iii] To provide data security.
iv] To provide access control.
v] To reduce the complexity involved in key management where the user can encrypt his/her private data.

IV. SOFTWARE DESIGN

A) Data flow diagram:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. A context diagram is a top level (also known as "Level 0") data flow diagram. It only contains one process node ("Process 0") that generalizes the function of the entire system in relationship to external entities. DFD Layers. ... Draw the context diagram first, followed by various layers of data flow diagrams. DFD Levels.

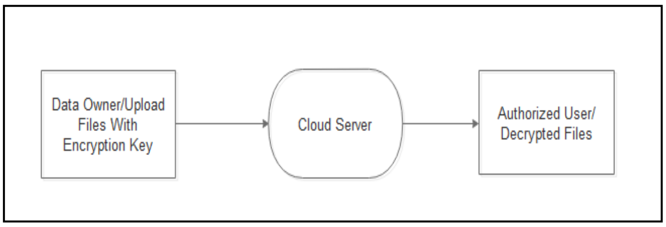
Data Owner/Upload Files With Encryption Key
Cloud Server
Authorized User/ Decrypted Files

Fig. Dataflow Diagram-level 0

1st Level DFD:

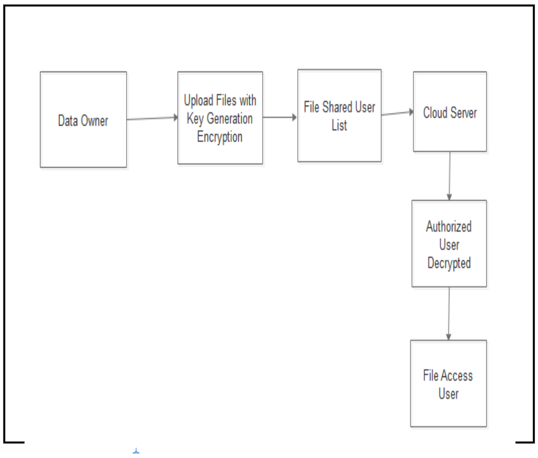
Data Owner
Upload Files with Key Generation Encryption
File Shared User List
Cloud Server
Authorized User Decrypted
File Access User

Fig. Dataflow Diagram-level

B) Flow Chart:

A flowchart is a diagram that depicts a process, system or computer algorithm. They are widely used in multiple fields to document, study, and plan, improve and communicate often complex processes in clear, easy-to understand diagrams.

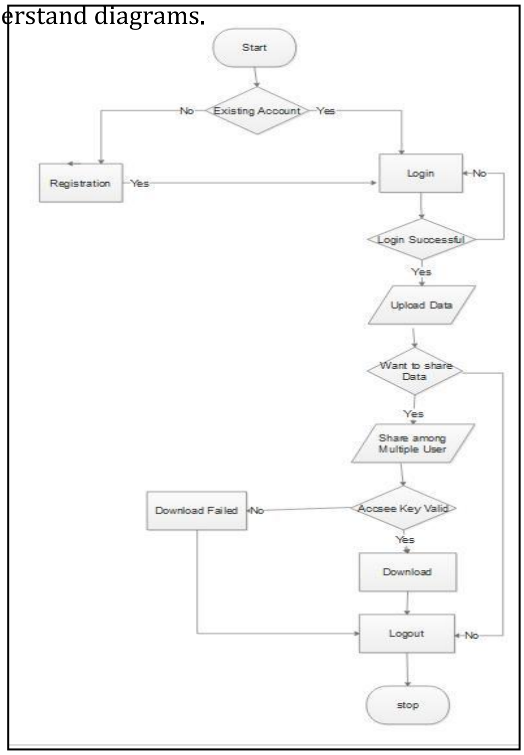

Fig.Flow Chart

V. IMPLEMENTATION DETAILS

Step 1: The application not only provides data content privacy but also includes identity privacy by using AnonyControl. AnonyControl decentralizes the central authority to hide the identity of origin and semi-anonymity is achieved with this. Subsequently, the AnonyControl-F, which entirely hides the identity, helps in attaining full anonymity.

Step 2: System uses Attribute Encryption Standard (AES) algorithm. The algorithm is used to protect classified information and is used by the entire world to encrypt and decrypt sensitive data. AES consists of three block ciphers. AES-128, AES-192, AES-256 and this each cipher uses 128 bits of blocks using cryptographic keys 128,192 and 256 bits to encrypt and decrypt delicate data. The ciphers installed in this algorithm uses. The same secret key for encrypting and decrypting.The different rounds of keys that is executed. Each series consists of steps that include substitution, transposition, and mixing of plain text. Then the plain text is transformed into cipher text.

Step 3: There are four types of systems: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and Data Consumer in one session. Data owner encrypts and uploads the files to the cloud server. Data consumer decrypts and downloads the files from the cloud server.

Step 4: To perform any operations on files and to have unlimited access to such records, the data owner and data consumer should first register in the application. When the registered at a time password, and unique id will send to their registered mail id.

Step 5: To upload and download files by the user. The user data owner/data consumer requests authority for permission. The authority provides public key to data owner and private key to the consumer. Issuing keys to authority and authentication in our system is succeeding using attribute-based encryption.

Step 6: Attribute-based encryption is a type of public-key encryption in which the secret User key and the cipher text are dependent upon (e.g., the country he lives, or the kind of Subscription he has). In such a system, the decryption of a cipher text is conceivable only if the set of attributes of the user key matches the attributes of the cipher text. A critical security aspect ofAttribute-Based Encryption is collusion-resistance. An adversary that holds multiple keys should be able to access data if at least one individual key grants access.

Step 7: The keys provided by the authority to the users (data owner and data consumer) can be used to perform operations and to have access to files in and out from the cloud server.

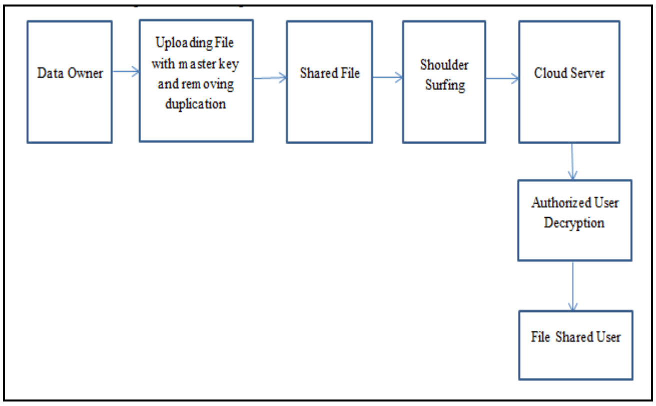
Data Owner
Uploading File with master key and removing duplication
Shared File
Shoulder Surfing
Cloud Server
Authorized User Decryption
File Shared User

Fig. Implementation details

A) Cloud Computing

Data privacy a lot of study has been done on the potential of cloud and the services that cloud computing can and could deal. These services can be characterized into four main sections: Storage as a Service (StaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS).Following section highlights these services and their usage in depth.

B) Storage as a Service:

Cloud offers a storage space that is huge, seemingly boundless, and rising every day. Storage as a Service (StaaS) allows cloud applications to gauge beyond their inadequate servers. Cloud storage systems needs to focus on requirements for upholding users' data and information, considering high performance, availability, replication, data reliability and reliability. The accountability to individual is maintained and upholds customers own computer storage as cloud vendors deal them the choice of loading their information in the cloud which is reachable whenever they need. Unfortunately, due to the contradictory nature of the necessities of cloud services, no one system implements all of them together.

C) Security Issues:

Companies are promptly moving onto cloud because they can now use the greatest capitals available on the market in the blink of an eye and also decrease their operations cost radically. But as more and more information is moved to the cloud the security concerns have continuing to grow. Data breaking is the biggest security issue. A capable hacker can easily get into a client side application and get into the client's intimate data .Incompetent and faulty APIs and interfaces become the target. IT companies which provide cloud services allow third party companies to alter the APIs and familiarize their own functionality which in turn allows these companies to comprehend the internal workings of the cloud. Denial of Service (DoS) is also a major menace wherein the user is approved partial or not at all access to their data. Companies now use cloud very frequently say all days and DoS can root huge increase in cost both for the user and service provider. Connection snooping is that in which a hacker can scan your online actions and copy/replay a particular broadcast to get into your private data. It can also lead to the user to unlawful or unsolicited sites. Data loss is also another issue.

C) Privacy Preservation

Trusted third party: an optional and neutral entity, which has advanced capabilities on behalf of the users, to perform data public auditing and dispute arbitration.

D) Shared authority

To address the above-mentioned privacy issue to propose privacy preserving authentication protocol (SAPA) for the cloud data storage based on cloud storage which gives authentication and authorization without conceding private information. The main consideration will be as follows: 1) A new privacy challenge in cloud storage is to be located and also to identify an in-direct privacy for data sharing, in which the challenged request itself cannot get the user's privacy 2) Design an authentication protocol which enhances a user's access request, which is related to the privacy. The shared access authority is achieved by unidentified access request matching mechanism. 3) Cipher text-policy is applied and a user can access its own data fields and proxy re-encryption is accepted to provide authorized data sharing among multiple users.

VI. CONCLUSIONS AND FUTURE SCOPE

In our Approach, in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

VII .ACKNOWLEDMENT

We would like to give the special thanks to the computer science engineering department of the college DACOE HOD Prof. Ashish N. Patil and Project guide Prof. Sayali P. Shinde to have their guidance. We are also thankful to the technologies that we have used to have such format of paper.

REFERENCES

[1]Hong Liu, Student Member, IEEE, HuanshengNing, Senior Member, IEEE, QingxuXiong,Member, IEEE,and Laurence T. Yang, Member, IEEE “Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing” IEEE Transactions on Parallel andDistributed Systems Volume: 26, Issue: 1, Jan. 2015.

[2] JingiLi,JinLi,DongqingXie and Zhang Cai " Secure Auditing and Deduplicating Data in Cloud" DOI 10.1109/TC.2015.2389960, IEEE Transactions on Computers

[3] Amol D Shelkar, Prof.Rucha R. Galgali, " Data Access Privilege With Attribute Based Encryption and User Revocation", International Research Journal of Engineering and Technology (IRJET), Nov 2016.

[4] Praveen N.R and Renju Samuel," Enhanced Efficient User Revocation Mechanism on Top of Anonymous Attribute Based Encryption" , International Journal of Emerging Technology in Computer Science Electronics, AUGUST 2016.

[5]M. Satishkumar,B. dayKumar,Ch.ArunKumar,"Attribute Based Data Sharing with At tribute Revocation to Control Cloud Data Access", International Journal of Computational Science, Mathematics and Engineering, February-2016.

[6] Muhammad YasirShabir, AsifIqbal, ZahidMahammad, and AtaullahGhafoor, " Analysis of Classical Encryption Techniques in Cloud Computing" , ISSN 1007-0214 09/10 pp102-119 Vol. 21, Number1, February